AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT AND SEARCH WARRANTS

I, TERRENCE DUPONT, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1.   I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since April 2013. I am currently assigned to the Economic Crimes squad with the Boston Division of the FBI. Prior to this assignment, I spent two years on the Health Care Fraud squad and four and a half years on the Philadelphia Division's Public Corruption squad. During my time in the FBI, I have participated in investigations relating to mail and wire fraud, money laundering, and aggravated identity theft. I have also been the affiant on numerous complaint and search warrant applications.

2.   I am currently investigating the following individuals (collectively, the "defendants") for various federal crimes, including mail fraud, wire fraud, and conspiracy to commit those crimes, in violation of Title 18, United States Code, Sections 1341, 1343 and 1349, respectively; aggravated identity theft, in violation of Title 18, United States Code, Section 1028A; and money laundering and conspiracy to commit money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957 (collectively, the "TARGET OFFENSES"):

     a.   PRISCILA BARBOSA, a Brazilian national residing in Saugus, Massachusetts;

     b.   EDVALDO ROCHA CABRAL, a Brazilian national residing in Lowell, Massachusetts;

     c.   CLOVIS KARDEKIS PLACIDO, a Brazilian national residing in Citrus Heights, California;

d.   Defendant D   , a Brazilian national formerly residing in Burlington, Massachusetts;

e.   GUILHERME DA SILVEIRA, a Brazilian national residing in Revere, Massachusetts;

f.   Defendant F   , a Brazilian national currently residing in Boca Raton, Florida, and who previously resided in Revere, Massachusetts;

g.   Defendant G   , a Brazilian national who previously resided in Revere, Massachusetts;

h.   FLAVIO CANDIDO DA SILVA, a Brazilian national residing in Revere, Massachusetts;

i.   ALTACYR DIAS GUIMARAES NETO, a Brazilian national residing in Kissimmee, Florida;

j.   Defendant J   , a Brazilian national residing in Daly City, California;

k.   Defendant K   , a Brazilian national residing in Daly City, California;

l.   Defendant L   , a Brazilian national residing in Hercules, California;

m.   BRUNO PROENCIO ABREU, a Brazilian national residing in Saugus, Massachusetts;

n.   JORDANO AUGUSTO LIMA GUIMARAES, a Brazilian national residing in Salem, Massachusetts;

o.   **Defendant O**   , a Brazilian national residing in

Shrewsbury, Massachusetts;

p.   ALESSANDRO FELIX DA FONSECA, a Brazilian national residing in

Revere, Massachusetts;

q.   **Defendant Q**   , a Brazilian national

residing in Watertown, Massachusetts; and

r.   **Defendant R**   , a Brazilian national residing in Wheeling,

Illinois.

3.   I make this affidavit in support of a criminal complaint charging the defendants

with conspiracy to commit wire fraud, in violation of Title 18, United States Code, Section 1349.

As set forth below, I have probable cause to believe that the defendants conspired with others

known and unknown: (1) to open driver accounts with various rideshare and delivery service

companies using stolen identities and/or falsified documents; and (2) to make money by renting

or selling those fraudulent accounts to individual drivers who might not otherwise qualify to drive

for those services, and by exploiting referral bonus programs offered by the companies.

4.   I also make this affidavit in support of an application for search warrants for the

following premises because there is probable cause to believe that they contain fruits, evidence,

and instrumentalities of the TARGET OFFENSES, as described in Attachment B:

a.   1205 Rock Wood Drive, Saugus, Massachusetts (the "BARBOSA/ABREU

RESIDENCE"), as described in Attachment A-1; and

b.   4 Stone Lane, Apt. 5139, Malden, Massachusetts (the "DA SILVA"

RESIDENCE), as described in Attachment A-2.

3

5.   The facts in this affidavit come from my personal observations, my training and experience, information obtained from other agents and witnesses, and my review of documents—including bank records, text messages and "chats" between and among the defendants, and other materials obtained through legal process and Court-authorized search warrants. This affidavit is intended to show simply that there is sufficient probable cause for the requested complaint and search warrants and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE TO BELIEVE THAT FEDERAL CRIMES WERE COMMITTED

Overview of the Conspiracy

6.   Beginning by at least 2019 and continuing through at least April 2021, in the District of Massachusetts and elsewhere, the defendants conspired with one another and with others known and unknown to create fraudulent driver accounts with multiple rideshare and delivery companies (the "Rideshare/Delivery Companies"), and to rent or sell the accounts to individuals who might not otherwise qualify to drive for those services. The evidence I have reviewed indicates that the scheme included the following:

a.   Obtaining images of victims' driver's licenses, or the information on victims' driver's licenses, and Social Security Numbers, from various sources including the DarkNet[1];

b.   Creating accounts to drive for the Rideshare/Delivery Companies using those stolen identifiers;

---

[1] The DarkNet is part of the Internet that is not indexed and consists of overlaying networks that use the public Internet but require unique software, configuration, or authorization to access, which is predominately designed to hide the identity of the user. Payment for goods and services on the DarkNet is usually through virtual currency like bitcoin, which is also designed to be anonymous.

c.   Renting or selling those accounts, including to people who might not otherwise qualify to drive for the Rideshare/Delivery Companies;

d.   Coordinating on prices charged to rent and sell accounts so as not to undercut each other's business;

e.   Sharing tips about how to circumvent the Rideshare/Delivery Companies' fraud detection systems;

f.   Causing the Rideshare/Delivery Companies to generate Internal Revenue Service Forms 1099 in the names of the identity theft victims for income they never earned, and attempting to divert those Forms 1099 from being sent to the victims;

g.   Using fake driver accounts for the purpose of referring other drivers to the Rideshare/Delivery Companies, and then collecting referral bonuses from the companies for additional fake accounts that the conspirators created;

h.   Utilizing global positioning system ("GPS") "spoofing" applications to "cut the line" for rides or deliveries, or to make it appear that trips were longer than they actually were, in order to obtain increased fares from the Rideshare/Delivery Companies, and selling this technology to drivers.

7.   In renting or selling accounts, the conspirators either had payments from the Rideshare/Delivery Companies deposited directly into their accounts, and then transferred the payments—less their cut—to the subjects using the fraudulent accounts, or they had payments deposited directly with the subjects using the fraudulent accounts, and collected weekly rental payments, usually between $250 and $300 per week for Rideshare Companies, and $150 per week for Delivery Companies. The conspirators charged more for fraudulent accounts for which they edited the driver's photograph onto the driver's license that they used to open the account.

8.   To date, investigators have identified more than 2,000 individuals whose identities were stolen and used as part of the scheme.

Background on the Rideshare/Delivery Companies

9.   Rideshare Company A is a ride-hailing company that connects drivers with riders via a mobile phone application ("app"). To become a driver for Rideshare Company A in Massachusetts, applicants must be at least 21 years old, have at least one year of driving history (three years if under age 23), and pass a motor vehicle and criminal background check. Drivers apply through Rideshare Company A's app or its website and provide, among other things, their name, date of birth, Social Security number, an image of their driver's license, automobile registration and insurance information, and a profile photo. Drivers must also pass a separate background check run by the Massachusetts Department of Public Utilities ("DPU"). Rideshare Company A stores the information applicants enter on servers which are located outside the District of Massachusetts.

10.   Delivery Company B is an online food ordering and delivery service. To become a driver for Delivery Company B in Massachusetts, drivers applying to deliver via automobile must be at least 18 years old, have at least one year of driving history, and pass a motor vehicle and criminal background check.[2] Drivers apply through Delivery Company B's app or its website and provide, among other things, their name, date of birth, Social Security number, and profile photo. Drivers applying to deliver via automobile must also provide an image of their driver's

---

[2] Some of the Delivery Companies allow drivers to deliver via bicycle or on foot in certain locations.

license. Delivery Company B stores the information applicants enter on servers which are located outside the District of Massachusetts.

11.   Rideshare Company C is a ride-hailing company that connects drivers with riders via a mobile phone app. To become a driver for Rideshare Company C in Massachusetts, applicants must be at least 25 years old, possess a valid driver's license, Social Security number, and vehicle insurance, have at least one year of driving history, and pass a motor vehicle and criminal background check. Drivers apply through Rideshare Company C's app or its website and provide, among other things, their name, date of birth, Social Security number, an image of their driver's license, their automobile insurance information, and a photo of themselves ("selfie"). Drivers must also pass a separate background check run by the DPU. Rideshare Company C stores the information applicants enter on servers located outside the District of Massachusetts and operated by Amazon Web Services.

12.   Delivery Company D is an online food ordering and delivery platform. To become a driver for Delivery Company D in Massachusetts, drivers applying to deliver via automobile must be at least 18 years old, have a valid Social Security number, and pass a motor vehicle and criminal background check. Drivers apply through Delivery Company D's website and provide, among other things, their name, date of birth, and Social Security number. Drivers applying to deliver via automobile must also provide their driver's license number (but not an image of their license). Delivery Company D stores the information applicants enter on servers located outside the District of Massachusetts and operated by Amazon Web Services.

13.   Delivery Company E is an online grocery delivery and pick-up service platform. To become a driver for Delivery Company E in Massachusetts, drivers must be at least 18 years old and pass a motor vehicle and criminal background check. Drivers apply through Delivery

Company E's website and provide, among other things, their name, date of birth, Social Security number, image of their driver's license, and a "selfie" photo. Delivery Company E stores the information applicants enter on servers located outside the District of Massachusetts and operated by Amazon Web Services.

14.   When a driver account is opened, the Rideshare/Delivery Companies generally collect metadata concerning, among other things, the device used to open the account, its location, the Internet Protocol ("IP") address used to submit the applicant's information, and whether the account was referred by another driver.

15.   Each of the Rideshare/Delivery Companies uses a third-party company to complete the motor vehicle and criminal background check on driver applicants. This company runs the motor vehicle and criminal background check based on the name, date of birth, and Social Security number provided by the driver applicant.

16.   The DPU also completes a two-part background check for rideshare drivers in Massachusetts. For Rideshare Company A and Rideshare Company C, the DPU runs its check based on the name, date of birth, driver's license number, and last six digits of the Social Security number provided by the driver applicant. The DPU completes follow-up background checks on all Rideshare Company A and Rideshare Company C drivers in Massachusetts every six months based on this same information.

17.   None of the Rideshare/Delivery Companies requires that the vehicles used for rides or deliveries be registered to the driver. It is not uncommon for drivers to use a vehicle registered to someone else.

18.   The Rideshare/Delivery Companies occasionally offer referral bonuses depending on market conditions. To earn a referral bonus, existing drivers who are in good standing can refer

another person to become a driver for the company. Once the referred driver completes a set number of trips, which varies by company and market, the referring driver (and, at some companies, the referred driver) can earn a bonus. The amount of the bonus depends on the company and the market and can be greater than $1,000.

20. One way that the Rideshare/Delivery Companies pay their drivers is via direct deposit.[3] Payments generally, but not always, appear on bank statements with the name of the driver who purportedly completed the trip or delivery.

20. The Rideshare/Delivery Companies utilize various fraud detection systems. For example, Rideshare Company A periodically requires drivers to upload "selfie" photos to the app, which are compared to the driver's profile and license images. The defendants and other conspirators attempted to circumvent these fraud detection systems in multiple ways, including by (a) editing the images on victim's licenses to depict the subject driving under the fraudulent account, rather than the victim, (b) having subjects who used the fraudulent accounts keep a printout of the victim's face with them to use when prompted for a "selfie," or (c) editing their own photo onto the victim's license and using GPS "spoofing" technology to make it appear the "selfie" they took matched the location of the subject driver when the subject was prompted to upload a "selfie."

WEMERSON DUTRA AGUIAR

21. AGUIAR's role in the scheme is described in my May 5, 2021 Affidavit in Support of Criminal Complaint and Search Warrant (the "May 5 Affidavit"), attached to this Affidavit as Exhibit 1.

---

[3] Some of the companies also offer a debit card option for payment.

22.   In the May 5 Affidavit, I stated, based on my review of draft summary translations of WhatsApp chats conducted predominantly in Portuguese between and among AGUIAR and various conspirators, that the conspirators used templates of various states' driver's licenses, editing the victims' information and importing photos of the drivers who rented or purchased the fraudulent accounts from them.[4] AGUIAR discussed manipulating driver's licenses with, among others, GUIMARAES NETO and Defendant J . For example, as set forth below, AGUIAR sent images of victims' driver's licenses to GUIMARAES NETO, and GUIMARAES NETO sent back three stock images of the edited licenses either resting on a wallet or being held in a hand. Likewise, as set forth below, Defendant J requested that AGUIAR send him a template for a Massachusetts driver's license so that he could use it to create bogus license images. Additionally, BARBOSA emailed AGUIAR an attachment with a file name "Connecticut driver's license.zip." While I have not been able to open the attachment to the email from BARBOSA, I am aware that, later that day, AGUIAR sent the same file via WhatsApp to another conspirator, and this file opens to an image of a Connecticut driver's license.

23.   AGUIAR also discussed creating fraudulent driver's accounts with GUIMARAES NETO and Defendant J , as further detailed below, and discussed exploiting referral bonuses with conspirators, including, as detailed herein, GUIMARAES NETO.

---

[4] WhatsApp is a text messaging application that provides users with end-to-end encryption, which means that a WhatsApp message is visible only to the sender and receiver of the message. WhatsApp also allows users to send and receive voice recordings. WhatsApp users typically use their phone number as their WhatsApp account number to send and receive messages through the application.

PRISCILA BARBOSA

24.   As part of the scheme, BARBOSA prepared and submitted applications using fraudulent identifiers; rented and sold driver accounts; purchased and traded driver's licenses, Social Security numbers, and driver's license templates; fraudulently obtained referral bonuses from the Rideshare/Delivery Companies; and exchanged information with other conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection systems.

25.   For example, information provided by Rideshare Company A indicates that on or about April 10, 2019, a bogus account in the name of Victim 3 ("Account 3A") was created by a device named "iPhone de Priscila Barbosa."[5] A "selfie" photo uploaded with the account appears to be BARBOSA, based on my review of the photograph of BARBOSA on her United States visa. Information provided by Delivery Company B indicates that on or about the same date, a driver account was created in the name of Victim 3 ("Account 3B"), containing a different "selfie" of BARBOSA. The driver's license associated with Accounts 3A and 3B appears to be a picture of Victim 3's actual license. BARBOSA and Victim 3 are similar in appearance. The vehicle associated with Accounts 3A and 3B was registered to BARBOSA and another individual at 1905 Founders Way, Saugus, Massachusetts. That address is located in the Residences at Stevens Pond apartment complex. According to records from the management company for the Residences at Stevens Pond, BARBOSA rented an apartment at a different address in the Residences at Stevens

---

[5] To avoid confusion, I have continued the victim numbering system from the May 5 Affidavit, which addressed Victim 1 and Victim 2. Account have been numbered to correspond to the number assigned to the victim in whose name the account was created. I have also continued the co-conspirator numbering system from the May 5 Affidavit, such that references to "CC-2" in the May 5 Affidavit concern to the same person referenced as "CC-2" in this Affidavit.

Pond complex in or about April 2019. According to location data that Rideshare Company A collected, a number of other suspected fraudulent accounts linked to the "iPhone de Priscila Barbosa" device were created in the vicinity of the Residences at Stevens Pond.

26.   In total, the "iPhone de Priscila Barbosa" device is linked to approximately 265 accounts at Rideshare Company A, including Account 1, discussed in the May 5 Affidavit, which is associated with AGUIAR. Specifically, an individual attempted to open a second account at Rideshare Company A in the name of Victim 1 using a vehicle registration that was also used with a driver account linked to the "iPhone de Priscila Barbosa" device. Rideshare Company A flagged this second account in Victim 1's name for suspected fraud before it could be opened.

27.   As another example, on or about April 11, 2019, an account was created with Delivery Company B ("Account 4") in the name of Victim 4. The "selfie" uploaded to Account 4 is the same picture of BARBOSA that was used for Account 3B. The email address associated with Account 4 is Prihbarbosa1985@icloud.com, the Apple ID associated with an iCloud account subscribed to BARBOSA (the "BARBOSA iCloud Account"). The driver's license uploaded with Account 4 appears to be similar to some of the stock images that were used for other fraudulent accounts, but with Victim 4's information and BARBOSA'S photo.

28.   As another example, on or about November 21, 2019, account in the name of Victim 5 was created with Rideshare Company A in the vicinity of Saugus, Massachusetts. The IP address associated with the creation of that account was the Comcast IP address 73.123.179.9. The same IP address was used to log into the BARBOSA iCloud Account and to a Venmo account

registered to BARBOSA.[6]   Victim 5 reported receiving an IRS Tax Form 1099 for income purportedly earned working for Rideshare Company A, despite the fact that Victim 5 never worked for Rideshare Company A.

29.   I have reviewed BARBOSA's iCloud account pursuant to a Court-authorized search warrant. Among other items, I located hundreds WhatsApp chats, mostly in Portuguese, in which BARBOSA corresponded with individuals seeking to rent or buy driver accounts.

30.   The BARBOSA iCloud Account also contained Excel spreadsheets listing names, email addresses, birthdates, Social Security numbers, and/or driver's license numbers for hundreds of individuals. Two tabs in one such spreadsheet were labeled with the names of Delivery Company D and Delivery Company E. Certain entries are labeled "aprovada" (Portuguese for "approved"), "suspenso" (Portuguese for "suspended"), "reprovado" (Portuguese for "failed"), or with the name of the company that runs background checks for the Rideshare/Delivery Companies.

31.   Certain names and email addresses appearing in the spreadsheets were used to open fraudulent driver accounts. For example, one email address (which includes part of Victim 6's name, which I have redacted with "X"), "XXXXXdd2003@protonmail.com," was used to open an account ("Account 6") with Delivery Company D in the name of Victim 6 on or about December 9, 2019.[7]   Account 6 was linked to BARBOSA'S Bank of America account. Bank statements indicate that, between January and May 2020, BARBOSA received $43,500 in deposits from Delivery Company D in the name of Victim 6. According to Delivery Company D's records,
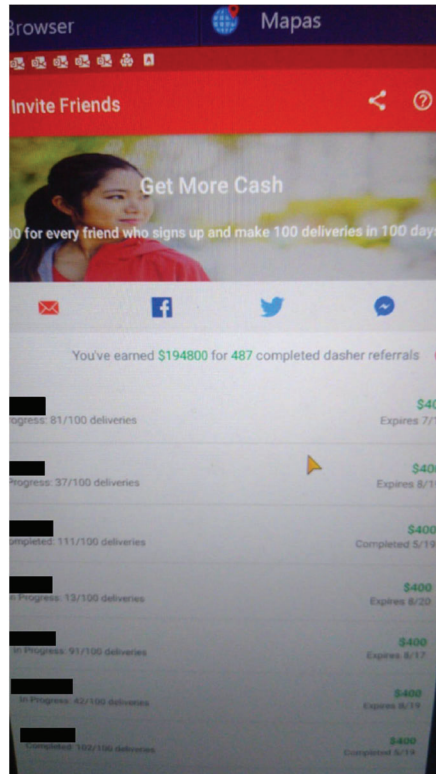
---

[6] Venmo is a mobile payment service owned by PayPal that allows account holders to transfer funds to others via a mobile phone application.

[7] ProtonMail is an encrypted email service.

Account 6 did not complete any deliveries. Rather, it appears Account 6 was created solely to receive payments from Delivery Company D's referral bonus program.

32.   The BARBOSA iCloud Account also contained items in the Notes app listing many similar email addresses structured as "[victim's name]dd[number]@protonmail.com" along with corresponding Social Security numbers, dates of birth, and passwords. Other Notes list names of drivers, the Rideshare/Delivery Companies for which BARBOSA created an account for that driver, and what appears to be the name of the conspirators with whom she shared the account, such as ABREU, Co-Conspirator 5 ("CC-5"), and others. Still other notes appear to contain instructions for how to circumvent the Rideshare/Delivery Companies fraud detection systems, such as instructions to delete machine "cookies" and delete and reinstall the app. The BARBOSA iCloud Account also contained hundreds of pictures of driver's licenses.

33.   On or about June 7, 2020, BARBOSA created a WhatsApp group that included herself, CABRAL, PLACIDO, ^{Defendant D}, DA SILVEIRA, and CC-5 that she named "Mafia." I have reviewed a computer-generated translation of this chat. This group discussed how to exploit referral bonuses. For example, on or about August 21, 2020, BARBOSA sent the following image to the "Mafia" group chat. The image, from which victims' names have been redacted, suggests that BARBOSA and her conspirators received $194,800 from Delivery Company D in connection with 487 referrals:

34.   Participants in the "Mafia" group chat also discussed Rideshare/Delivery Company

accounts rented or sold to drivers, including ways to apply for accounts to improve the likelihood

of the Rideshare/Delivery Company approving the account, issues with the Rideshare/Delivery

Companies closing accounts, and vetting potential purchasers of the accounts. They also discussed

ways to take advantage of the Rideshare/Delivery Companies' platforms and increase their profits

from the scheme. For example, in or about June 2020, BARBOSA, CABRAL, DA SILVEIRA,

COLACO, and CC-5 purchased a "bot" to enable them to "cut the line" to grab batches of

deliveries on Delivery Company E's app.[8] Both [Defendant D] and CC-5 sent BARBOSA $1,000 via

Venmo for the "bot," with CC-5 adding a picture of a robot to his payment. Upon purchasing the

---

[8] A "bot" is a software application that runs automated tasks over the Internet.

program, CABRAL tested it and advised the others, in substance, that if he could use the program, anyone could. CABRAL directed that they charge drivers $500 for the "bot."

35.   The members of the "Mafia" chat group also shared ways to advertise their "business," exchanged images of driver's licenses, and discussed ways to get around the Rideshare/Delivery Companies' fraud detection systems, such as by using a virtual private network ("VPN") to avoid detection of their IP address.[9]

36.   BARBOSA purchased and traded driver's licenses with numerous conspirators, including ABREU, Defendant O, LIMA GUIMARAES, and CC-2. Additionally, I have probable cause to believe that BARBOSA purchased Social Security numbers on the DarkNet. For example, on or about November 18, 2019, BARBOSA asked ABREU, in substance, to teach her how to buy Bitcoin after she discovered a site to purchase Social Security numbers that required payment in Bitcoin. On or about October 29, 2020, BARBOSA sent   Defendant Q   a photo of her computer opened to a DarkNet site where she was looking for the Social Security number of Victim 7.

37.   I have reviewed a bank account in BARBOSA'S name at Bank of America. The address associated with the account is 1205 Rock Wood Drive, Saugus, Massachusetts, another address in the Residences at Stevens Pond complex. Between on or about June 12, 2019 and on or about January 11, 2021, approximately $782,340 was deposited into BARBOSA'S Bank of

---

[9] A VPN creates a secure, encrypted connection between a computer and a VPN server located elsewhere and can be used to hide a user's computer IP address by replacing it with the VPN provider's IP address.

America account.   Zelle transfers accounted for approximately $402,248 of that amount.[10]

Payments from several of the Rideshare/Delivery Companies for completed rides accounted for approximately $248,076.   These companies paid BARBOSA approximately $201,940 for trips completed under at least 68 names other than her own name.

38.   For example, between January and May 2020, BARBOSA received $20,623.16 in deposits from Rideshare Company A in the name of Victim 8. According to Rideshare Company A's records, the account in the name of Victim 8 ("Account 8") was created with a Florida driver's license in Victim 8's name. A "selfie" of an individual that appears to match the picture on the driver's license was uploaded to Account 8. BARBOSA'S bank statement reflects a pattern of receiving a payment from Rideshare Company A in the name of Victim 8 and transferring a similar amount of money, less approximately $100-$200, to another individual, Co-Conspirator 6 ("CC-6"), on the same day. Based on my knowledge of the investigation, I believe that CC-6 rented Account 8 from BARBOSA, and that BARBOSA collected the proceeds from CC-6's trips in her account and then transferred the money, less her rental fee, to CC-6.

39.   Between approximately June 2019 and September 2020, BARBOSA received approximately $302,599 in Zelle transfers. These transfers typically were in amounts between $100 to $300. Based on my knowledge of this investigation, I believe that many of these transfers were from individuals renting or buying fraudulent driver accounts.

---

[10] Zelle is a digital payment network owned by a group of banks, including Bank of America and Wells Fargo, among others. Zelle allows users to send and receive money, typically over a mobile device, directly from their bank accounts at participating banks.

EDVALDO ROCHA CABRAL

40.   The investigation has revealed that, as part of the scheme, CABRAL advertised the conspirators' scheme to potential drivers; prepared and submitted applications using fraudulent identifiers; rented and sold driver accounts; fraudulently obtained referral bonuses from the Rideshare/Delivery Companies; supplied victims' driver's licenses to conspirators; and exchanged information with other conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection systems.

41.   CABRAL communicated with BARBOSA and the "Mafia" group via WhatsApp at the phone number 786-583-7765 (the "CABRAL TELEPHONE 1"). The profile photo for the WhatsApp account associated with the CABRAL TELEPHONE 1 is a photo of CABRAL with a woman. Additionally, BARBOSA entered the CABRAL TELEPHONE 1 into her contacts under the name "Ed."

42.   CABRAL also communicated with BARBOSA via WhatsApp at the phone number 781-797-0564 (the "CABRAL TELEPHONE 2"). I have listened to voice messages sent from both the CABRAL TELEPHONE 1 and the CABRAL TELEPHONE 2. Both have the same, distinctive voice. BARBOSA entered the CABRAL TELEPHONE 2 into her contacts under the name "Edd." Both the CABRAL TELEPHONE 1 and the CABRAL TELEPHONE 2 are in the "Mafia" group chat. In that chat, BARBOSA told the others that "Ed" was in the chat under two different phone numbers.

43.   In the "Mafia" chat group, CABRAL and BARBOSA shared his advertisements for their scheme with the other members of the group.

44.   As noted above, the group purchased a "bot" for "cutting the line" to grab batches from Delivery Company E. On or about June 8, 2020, CABRAL confirmed to the "Mafia" group
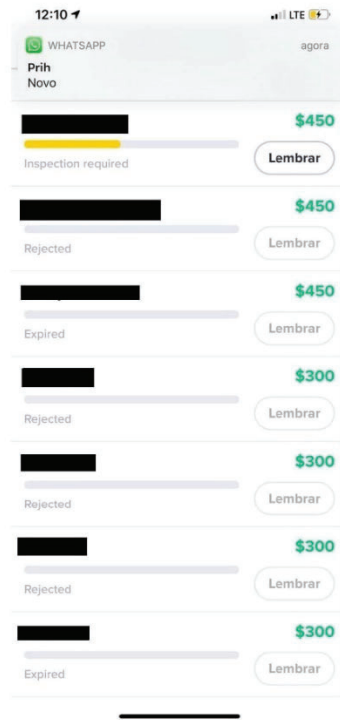
that he had agreements to sell the "bot" to several people. CABRAL suggested that ^{Defendant D} create a video to share with the individuals to whom they rented and sold accounts showing the features of the "bot."

45.   CABRAL and BARBOSA also had separate WhatsApp chats with each other, during which CABRAL used both the CABRAL TELEPHONE 1 and CABRAL TELEPHONE 2. I have reviewed computer-generated translations of these chats. The chats make clear that CABRAL and BARBOSA worked together to create and rent fraudulent driver accounts. For example, on or about October 25, 2019, CABRAL and BARBOSA discussed, in substance, that Rideshare Company C had approved one of their accounts, in the name of Victim 9. On or about October 28, 2019, CABRAL and BARBOSA discussed, in substance, that an account they created for another individual, Co-Conspirator 7 ("CC-7"), had been approved, and CABRAL notified CC-7. CABRAL and BARBOSA also discussed payments they were owed for their accounts and that they owed each other. CABRAL also advertised the accounts he and BARBOSA shared. For example, on October 29, 2019, BARBOSA notified CABRAL that she had a female account with Delivery Company B available, and CABRAL said he would advertise it.

46.   CABRAL and BARBOSA also shared the proceeds of some of their fake driver accounts with CC-5. For example, on or about November 10, 2019, BARBOSA and CABRAL discussed, in substance, sharing an account with CC-5 and dividing the rental payments by three.

47.   BARBOSA and CABRAL also discussed the referral bonuses they were getting from setting up fake accounts. For instance, on or about October 31, 2019, CABRAL and BARBOSA discussed, in substance, using a referral code for Rideshare Company C and splitting the referral bonus. In another instance, on or about November 6, 2019, BARBOSA sent CABRAL the screenshot set forth below (from which I have redacted victim names) depicting a list of driver

accounts BARBOSA and CABRAL had referred to Rideshare Company C and showing their

progress toward earning the referral bonus:

48.   CABRAL also created his own accounts and relied on BARBOSA to help him

answer the identity verification questions asked during the application process. To help her answer

the questions, CABRAL shared with BARBOSA photos of the victims' licenses and their Social

Security numbers. CABRAL also shared images of his computer with BARBOSA, which appear

to show other fraudulent driver accounts he was managing.

49.   CABRAL often supplied BARBOSA with victims' information. For example, on

or about November 9, 2020, CABRAL sent BARBOSA a list of victim names, addresses, dates of

birth, and Social Security numbers.   He also purchased driver's licenses from BARBOSA

occasionally. For example, on or about December 10, 2020, BARBOSA sent CABRAL five

images of driver's licenses, and instructed him to pay $175 to the telephone number 857-888-2714

via Zelle. As set forth below, this phone number belongs to LIMA GUIMARAES. Additionally,

I have seen a WhatsApp chat between LIMA GUIMARAES and BARBOSA from the prior day in which LIMA GUIMARAES sent BARBOSA the same five images. Accordingly, based on my training and experience and my knowledge of this investigation, I believe that BARBOSA acted as a middleman in the sale of the five victim licenses from LIMA GUIMARAES to CABRAL.

50.   BARBOSA and CABRAL also shared tips and resources, including the name of a contact who could edit licenses for them. On or about November 19, 2019, CABRAL asked BARBOSA if there was an app that could help him manage multiple ProtonMail accounts. Based on my involvement in this investigation, I am aware that many of the defendants, including BARBOSA and AGUIAR, used ProtonMail to create email accounts for use with the driver accounts they created. Based on my training and experience, I am aware that ProtonMail is an encrypted email service. Accordingly, I believe the conspirators used this service as a means to avoid detection of their scheme.

51.   I have reviewed a bank account in CABRAL's name at Bank of America. The address associated with the account is 60 Linwood Street, Apt. 1, Malden, Massachusetts, an address that is also associated with bank records for CC-5. Between on or about June 6, 2019 and on or about January 5, 2021, approximately $623,721 was deposited into CABRAL's Bank of America account. Zelle transfers accounted for approximately $315,695 of that amount. Many of those Zelle transfers reference the name of Rideshare Company C. Payments from several of the Rideshare/Delivery Companies accounted for approximately $26,964. Of these, many of the payments are round numbers, which suggests to me that they are referral bonuses.

CLOVIS KARDEKIS PLACIDO

52.   The investigation has revealed that, as part of the scheme, PLACIDO edited driver's licenses; prepared and submitted applications using fraudulent identifiers; rented and sold

driver accounts; fraudulently obtained referral bonuses from the Rideshare/Delivery Companies; and exchanged information with other conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection systems.

53.   PLACIDO communicated with BARBOSA and the "Mafia" group via WhatsApp at the phone number 407-820-7640 (the "PLACIDO TELEPHONE"). I have reviewed computer-generated translations of these chats. In the chat with BARBOSA, PLACIDO sent pictures of himself to BARBOSA as well as an image of his driver's license. Additionally, BARBOSA saved the PLACIDO TELEPHONE in her contacts under the name "Clovis."

54.   On or about April 9, 2020, PLACIDO offered to sell BARBOSA information and a link regarding referral bonuses available through Delivery Company D. After some negotiations, BARBOSA agreed to pay PLACIDO $1,000 for the information and link. In connection with this exchange, PLACIDO sent BARBOSA the link, created an account with Delivery Company D using Victim 10's information, and, after receiving the $1,000 payment from BARBOSA, sent BARBOSA an image of Victim 10's license and the log-in information for the account, as well as the zip code to use when applying to maximize the referral bonus.

55.   PLACIDO and BARBOSA also exchanged tips about how to circumvent security measures employed by the Rideshare/Delivery Companies. For example, on or about April 9, 2020, PLACIDO instructed BARBOSA how to get past the background check for Delivery Company D to deliver with a scooter, rather than a car. On or about April 10, 2020, PLACIDO shared with BARBOSA that he managed to solve an error she was experiencing by uninstalling and reinstalling Delivery Company D's app. On or about April 15, 2020, BARBOSA explained to PLACIDO that it was better to use ProtonMail than using Gmail to register email addresses for fake accounts.

56.   PLACIDO also told BARBOSA, in substance, that he was creating fraudulent accounts. On or about April 10, 2020, PLACIDO stated that he had created 16 driver accounts the previous day, after BARBOSA responded that she had created 21 accounts.

57.   PLACIDO also referred drivers to BARBOSA. On or about April 11, 2020, PLACIDO sent the contact information of a driver looking for an account with Delivery Company E to BARBOSA.

58.   After BARBOSA created the "Mafia" group, PLACIDO also exchanged tips with his fellow "Mafia" group members, including regarding which markets were accepting new accounts and where to secure higher referral bonuses. For example, on or about October 22, 2020, PLACIDO shared, in substance, that despite using a VPN to hide his location, he had been unsuccessful in opening driver accounts in Canadian markets. He also explained that he used the VPN to disguise himself when browsing the DarkNet.

59.   PLACIDO also edited driver's license images. For example, on or about January 29, 2021, PLACIDO sent BARBOSA a photo of his computer, opened to a photo editing application, with an image of Victim 12's driver's license displayed, but with PLACIDO's face edited into the license. PLACIDO asked BARBOSA if she thought the image would pass the background check process for Delivery Company E, despite the fact that it was missing one of the security features.

Defendant D

60.   The investigation has revealed that, as part of the scheme, [Defendant D] rented and sold driver accounts; fraudulently obtained referral bonuses from the Rideshare/Delivery Companies; sold and installed "bots" for use in connection with the Rideshare/Delivery Company apps; and

exchanged information with other conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection systems.

61.   ^{Defendant D} communicated with BARBOSA and the "Mafia" group via WhatsApp at the phone number ███████ (the "^{Defendant D} TELEPHONE"). I have reviewed computer-generated translations of these chats. In the chats, BARBOSA and ^{Defendant D} sent screenshots confirming that they sent funds to each other. I have reviewed Bank of America records for ^{Defendant D} that reflect corresponding transfers in an account in her name. Additionally, BARBOSA saved the ^{Defendant D} TELEPHONE in her contacts under the name "Defendant D."

62.   In the WhatsApp chats between ^{Defendant D} and BARBOSA, they exchanged information about the Rideshare/Delivery Company apps and how to create and maintain fraudulent driver accounts. ^{Defendant D} and BARBOSA also exchanged photographs of both real and altered driver's licenses. They also coordinated about the receipt and use of debit cards in connection with one of the Rideshare/Delivery Company apps.

63.   BARBOSA and ^{Defendant D} shared earnings from their fraudulent driver account activity. For example, on or about January 7, 2020, BARBOSA notified ^{Defendant D} that she was sharing $450 from a referral bonus for one of the Rideshare/Delivery Companies, less $50 for the account that used another conspirators's photograph. ^{Defendant D}'s bank records for her Bank of America account ending in x8995 reflect a corresponding transfer from BARBOSA for $400 on or about January 7, 2020.

64.   ^{Defendant D} also communicated with other conspirators in the "Mafia" group chat. After BARBOSA created the "Mafia" group on or about June 7, 2020, ^{Defendant D} commented, "Caramba somos tão honesto para o nome do grupo ser esse," which I understand to mean, "Damn, we're so honest for the group's name to be that."

65.   The following day, ^{Defendant D} asked the group how much they would charge an individual for an account and a "bot" together; group participants then discussed a price. ^{Defendant D} indicated to the group that she knew of potential buyers for the "bot." As noted above, ^{Defendant D} transferred $1,000 via Venmo as her share for the purchase of the "bot."

66.   In various messages with the "Mafia" group, ^{Defendant D} described how to install the "bot" to work in connection with the Delivery Company E app, including how to install the "bot" on a phone remotely. ^{Defendant D} also troubleshot various "bot" installation problems raised by the other group members and managed email addresses and passwords used by the group in connection with the apps.

67.   ^{Defendant D} also discussed account rentals and deactivations with the "Mafia" group. In various messages, she asked group members whether they had accounts available to rent to individuals who had contacted her for accounts. In other messages, she and other group members speculated about why one Rideshare/Delivery company had deactivated accounts that had accrued referral bonuses. On or about August 22, 2020, ^{Defendant D} sent a screenshot of an email from Delivery Company D, addressed to Victim 13, in which Delivery Company D apologized for "mistakenly" deactivating the account "for referral fraud."

68.   As noted, I have reviewed a bank account in ^{Defendant D}'s name at Bank of America. Between in or around March 2019 and in or around December 2020, ^{Defendant D} received deposits of approximately $82,661 from Rideshare/Delivery Companies. Payments for at least $44,760 of this amount specifically referenced the names of at least 53 other individuals, while other payments referenced no driver name. During this period, ^{Defendant D} also received Zelle transfers totaling over $60,000, including recurring Zelle transfers from numerous individuals. Based on my knowledge

of this investigation, I believe that many of these transfers were from individuals renting or buying

fraudulent driver accounts and/or purchasing "bots" to use with such accounts.

GUILHERME DA SILVEIRA

69.   The investigation has revealed that, as part of the scheme, DA SILVEIRA obtained

driver's license images; rented and sold fraudulent driver accounts; fraudulently obtained referral

bonuses from the Rideshare/Delivery Companies; and exchanged information with other

conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection

systems.

70.   DA SILVEIRA communicated with BARBOSA and the "Mafia" group via

WhatsApp using the phone number 857-346-7961 (the "DA SILVEIRA TELEPHONE"). I have

reviewed computer-generated translations of these chats. In the chat with BARBOSA, DA

SILVEIRA sent pictures of himself to BARBOSA, and BARBOSA sent screenshots confirming

she sent funds to DA SILVEIRA. I have reviewed Bank of America records for DA SILVEIRA

that reflect corresponding transfers in an account in his name. Additionally, BARBOSA saved the

DA SILVEIRA TELEPHONE in her contacts under the name "Guiii." DA SILVEIRA also

communicated with AGUIAR via WhatsApp using the DA SILVEIRA TELEPHONE. AGUIAR

saved the DA SILVEIRA TELEPHONE in his contacts under the name "Guilherme Alug Fusion."

I believe, based on my knowledge of this investigation, that "Alug Fusion" is a reference to DA

SILVEIRA'S rental of a Ford Fusion from AGUIAR, as I understand "alug" is the Portuguese

word for "rent."

71.   WhatsApp messages between BARBOSA and DA SILVEIRA indicate that DA

SILVEIRA provided driver's license images to BARBOSA for the purpose of opening driver

accounts with multiple Rideshare/Delivery Companies with fraudulent identifiers.

72.   DA SILVEIRA was also part of the "Mafia" group chat. Among other activity in the chat, DA SILVEIRA sent photos of his phone as he was attempting to access the "bot" the group purchased. DA SILVEIRA also complained, in substance, that drivers to whom he had rented or sold accounts were coming to him with problems related to their accounts.

73.   I have also reviewed draft summary translations of WhatsApp messages between AGUIAR and CC-2. In those chats, they discuss, in substance, that DA SILVEIRA supplied CC-2 with driver's license images for the purpose of opening fraudulent driver accounts with Rideshare/Delivery Companies. For example, on or about December 13, 2019, CC-2 told AGUIAR that DA SILVEIRA had provided CC-2 eight "clean" California driver's licenses for the purpose of obtaining fraudulent accounts with Delivery Company B, and that CC-2 and DA SILVEIRA would split the profits generated by the use of those fraudulent accounts, and invited CC-2 to use the same driver's licenses to apply for accounts with Rideshare Company A. CC-2 indicated in other messages with AGUIAR that CC-2 and DA SILVEIRA maintained an arrangement pursuant to which DA SILVEIRA provided driver's licenses, CC-2 obtained Social Security numbers and edited images of the licenses, and CC-2 and DA SILVEIRA shared the profits.

74.   Additionally, as of March 3, 2021, DA SILVEIRA had at least nine vehicles registered in his name at the address 14 Woodman Way, Apartment 9, Newburyport, Massachusetts. DA SILVEIRA'S domestic partner had at least nine additional vehicles registered in her name at the same address. Based on my training and experience and knowledge of the investigation, I believe that DA SILVEIRA rented these vehicles to individuals driving for Rideshare/Delivery Companies under fraudulent accounts.

75.   I have reviewed a bank account in DA SILVEIRA'S name at Bank of America. The address associated with the account is 93 Ward Street in Revere, Massachusetts, which I know to be an address where DA SILVEIRA resides. Between on or about June 25, 2019 and on or about December 24, 2020, DA SILVEIRA received a total of approximately $106,842 in payments from various Rideshare/Delivery Companies that referenced at least 37 other individuals' names. Some of these names were used by other conspirators to create fraudulent accounts. Based on my knowledge of the investigation, I believe that DA SILVEIRA received these payments for renting out accounts fraudulently opened in these individuals' names.

76.   DA SILVEIRA'S bank statements for that period reflected Zelle inflows totaling $225,107, which is consistent with the amount of Zelle inflows for other conspirators renting and selling fake driver accounts. Zelle account statements reflect payments totaling approximately $7,096 from BARBOSA and approximately $2,052 from CC-2. DA SILVEIRA also transferred approximately $4,090 to AGUIAR.

Defendant F

77.   The investigation has revealed that, as part of the scheme, ^{Defendant F} prepared and submitted applications using fraudulent identifiers; rented and sold fraudulent driver accounts; purchased and traded driver's licenses and Social Security numbers; sold GPS "spoofing" technology to drivers; and exchanged information with other conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection systems.

78.   A number of the driver accounts associated with AGUIAR and BARBOSA appear to have been created using stock driver's license images, including a stock image in which a driver's license rests on a wallet. Metadata that Rideshare Company A collected for several of

these accounts indicates that the images were uploaded in the vicinity of Overlook Ridge in Revere, Massachusetts. I am aware that ^{Defendant F} previously resided at 19 Overlook Ridge.

79.   For example, on or about March 5, 2020, an account with Rideshare Company A in the name of Victim 14 ("Account 14") was created in the vicinity of Overlook Ridge. GPS data placed the driver using the account in the area of Overlook Ridge at times when the driver was not completing trips. Account 14 is associated with telephone number ███████ (the "^{Defendant F} TELEPHONE"), which is same telephone number associated with ^{Defendant F}'S iCloud account and with WhatsApp chats between AGUIAR and an individual believed to be ^{Defendant F}, who is identified in AGUIAR's contacts as "^{Defendant F}."   Additionally, the driver's license image associated with Account 14 bears the photo of ^{Defendant F}.

80.   Rideshare Company A has identified approximately ten other fraudulent accounts with driver's license images bearing ^{Defendant F}'S image (the "^{Defendant F} Accounts"). Many of the ^{Defendant F} Accounts are linked to a vehicle registered to Co-Conspirator 8 ("CC-8"), an individual with a Rideshare Company A account who referred some of the ^{Defendant F} Accounts to Rideshare Company A. I have reviewed draft summary translations of WhatsApp messages between AGUIAR and ^{Defendant F} obtained through a Court-authorized search warrant, and am aware that five accounts identified by Rideshare Company A as linked to CC-8's account were created for ^{Defendant F} by AGUIAR. Those messages indicate, in substance, that ^{Defendant F} sent AGUIAR driver's license images for these five accounts; that AGUIAR obtained the corresponding Social Security numbers to be used with these five accounts; and that ^{Defendant F} sent $1,000 via Zelle to

AGUIAR with the note "SS," which I believe, based on my training and experience and my knowledge of this investigation, refers to "Social Security."[11]

81.   In or about October 2020, ten accounts with Delivery Company B were created in the names of ten different victims from the Comcast IP Address 73.123.253.111. The profile photographs and driver's license images uploaded for these accounts bear the image of Defendant F or Defendant G. IP Address 73.123.253.111 is a Comcast IP address subscribed to Defendant F at 19 Overlook Ridge Terrace, Apartment 204, in Revere, Massachusetts and is associated with the Defendant F TELEPHONE. Delivery Company B has identified additional fraudulent accounts that were created from this same IP address. According to the GPS data collected by Delivery Company B, one of these accounts was active in the vicinity of Overlook Ridge.

82.   In WhatsApp chats with AGUIAR, Defendant F exchanged driver's licenses, Social Security numbers, and information about how to get accounts approved. Defendant F also told AGUIAR that he had obtained a GPS "spoofing" application to, in substance, make rides appear longer than they were, in order to secure a higher fare. Defendant F told AGUIAR he was selling the "spoofing" app to drivers.

83.   Additionally, in or about March 2020, Defendant F referred another individual, Co-Conspirator 9 ("CC-9"), to AGUIAR as someone who could edit driver's licenses. AGUIAR sent the Connecticut license template he received from BARBOSA to CC-9.

---

[11] The $1,000 transfer came from an account in the name of another female individual ("Subject 1"). Defendant F sent AGUIAR a photo of the confirmation that he had sent the $1,000 payment on or about February 23, 2020. The only payment for $1,000 to AGUIAR on that date was from Subject 1. Other payments from Defendant F to AGUIAR were also sent from Subject 1's account. In WhatsApp chats, Defendant F also told AGUIAR that he used his girlfriend's account to send payments.

Defendant G

84. The investigation has revealed that, as part of the scheme, Defendant G prepared and submitted applications using fraudulent identifiers; rented and sold fraudulent driver accounts; purchased and traded Social Security numbers; and exchanged information with other conspirators on prices for Social Security numbers.

85. Rideshare Company A identified approximately seven fraudulent accounts created between on or about December 2019 and on or about October 2020 with driver's license images bearing Defendant G's image (the "Defendant G Accounts"). At least three of the Defendant G Accounts are linked to a vehicle registered to Defendant G. Additionally, these three accounts feature stock images of a license in a hand, which appear to be the same stock images associated with some of the Defendant F Accounts. Further, CC-8, who referred many of the Defendant F Accounts, also referred one of the Defendant G Accounts to Rideshare Company A under its driver referral bonus program. Two of the accounts were created using the IP address 73.123.253.111, which, as previously noted, was subscribed to Defendant F.

86. Defendant G also received payments from the Rideshare/Delivery Companies in the names of at least three individuals, and more than $40,000 in payments where the driver was not attributed. He also received a $150 Zelle payment in or about September 2018 with the description "Conta [Delivery Company D]," which I believe based on my knowledge of the investigation is a rental payment for an account with Delivery Company D. I understand that "conta" is the Portuguese word for "account."

87. Defendant G was also a member of a group WhatsApp chat that included AGUIAR, Defendant F, and others, in which he offered accounts for sale. For example, on or about September 10, 2020, Defendant G notified the group that he had a delivery account available in

the Worcester, Massachusetts area. On the same day, an account with Rideshare Company A in the name of Victim 15, with an address in Worcester, was created with Defendant G's image on the license.

88.   On or about February 9, 2020, Defendant G contacted AGUIAR over WhatsApp using the telephone number ▆▆▆▆▆▆▆ (the "Defendant G TELEPHONE"). The Defendant G TELEPHONE was registered with the management company in connection with Defendant G 's former residence in Revere, Massachusetts.

89.   I have reviewed a draft summary translation of the WhatsApp chat between Defendant G and AGUIAR. In the chat, Defendant G introduced himself to AGUIAR as " Defendant ," a friend of "Will" and "Flávio." I believe based on my knowledge of the investigation that "Flávio" is a reference to DA SILVA, whose first name is "FLAVIO." In substance, Defendant G asked AGUIAR if he could get Social Security numbers for him based on a driver's license image. In the chat, Defendant G referenced a price AGUIAR had quoted Defendant F for Social Security numbers. Thereafter, on or about February 18, 2020, Defendant G sent AGUIAR a photo of a driver's license of Victim 16, and, after Defendant G transferred $250 to AGUIAR, with the memo "Dutra Ssn," AGUIAR sent Defendant G Victim 16's Social Security number. AGUIAR identified himself by his middle name, "DUTRA," on WhatsApp. On or about April 20, 2020, a Rideshare Company A account was created in the name of Victim 16, after receiving a referral from CC-8.

90.   I have reviewed bank and Zelle records for Defendant G. The records reflect a number of $50 transfers from BARBOSA in or about December 2019, as well as a $1,179 transfer in or about October 2019. Defendant G also received funds from and sent money to DA SILVA

and ^{Defendant F}. Defendant G also received payments from Rideshare Company C in the names of three different individuals.

FLAVIO CANDIDO DA SILVA

91.   The investigation has revealed that, as part of the scheme, DA SILVA rented and sold driver accounts and referred other conspirators to AGUIAR.

92.   In total, investigators have identified at least 19 fraudulent driver accounts with DA SILVA's photograph on the driver's license, under the names of at least 11 individuals. The "selfie" associated with each of these accounts is a photo of DA SILVA.

93.   I have reviewed bank and Zelle records for DA SILVA. The records reflect payments to DA SILVA from Rideshare/Delivery companies totaling approximately $37,746 between June 2019 and December 2020, including payments totaling approximately $12,919 that specifically referenced the names of at least 14 other individuals. DA SILVA also received numerous Zelle transfers from individuals in amounts ranging from $100 to $300, which I believe based on my knowledge of the investigation are rental payments to DA SILVA for fraudulent driver accounts. In total, between in or about June 2019 through in or about December 2020, DA SILVA received approximately $200,263 in Zelle inflows.

94.   Bank statements also reflect numerous Zelle and PayPal transfers between DA SILVA and ^{Defendant F}, as well as recurring Zelle transfers from Defendant G in varying amounts. WhatsApp messages between AGUIAR, Defendant G, and ^{Defendant F} indicate that DA SILVA referred Defendant G to AGUIAR in or about February 2020 to obtain Social Security numbers, and that AGUIAR made a $150 Zelle transfer in April 2020 to DA SILVA, whom AGUIAR identified in his contacts as "Flavio Santa Fe." The WhatsApp profile photo for the "Flavio Santa Fe" account appears to match known photographs of DA SILVA.

ALTACYR DIAS GUIMARAES NETO

95.   The investigation has revealed that, as part of the scheme, GUIMARAES NETO acted as a middleman for Co-Conspirator 10 ("CC-10"), another participant in the scheme who edited driver's licenses. GUIMARAES NETO also rented and sold fraudulent driver accounts and exchanged information with other conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection systems.

96.   In a WhatsApp chat on or about October 16, 2019, AGUIAR asked another conspirator, CC-5, for the contact information for the person who edits driver's licenses. CC-5 forwarded AGUIAR the contact information for "Altacyr [delivery company]" with a phone number of 857-505-5848 (the "GUIMARAES NETO TELEPHONE") and told AGUIAR that he would need to make an upfront payment of $40 per license.

97.   On or about the same day, AGUIAR contacted, via WhatsApp, a person identified in AGUIAR's contacts as "Altacyr [delivery company]" at the GUIMARAES NETO TELEPHONE. The GUIMARAES NETO TELEPHONE is associated with a Zelle account belonging to GUIMARAES NETO, which is linked to a Bank of America account in the name of GUIMARAES NETO.

98.   I have reviewed a draft summary translation of the WhatsApp chat between GUIMARAES NETO and AGUIAR. During their initial communication, GUIMARAES NETO indicated to AGUIAR that it was his friend, CC-10, edited driver's licenses and charged $40 for that service. GUIMARAES NETO and AGUIAR also discussed, in substance, that AGUIAR shared accounts with CC-5 and that GUIMARAES NETO had previously had problems with CC-5. GUIMARAES NETO offered to collaborate with AGUIAR.

99.   Thereafter, between in or about October 16, 2019 and November 8, 2019, AGUIAR sent GUIMARAES NETO approximately 20 passport-style photos and images of victim's driver's licenses, and in return, GUIMARAES NETO sent AGUIAR images of correspondingly altered licenses. All of the images GUIMARAES NETO sent to AGUIAR were the same three stock images, but with different victim's licenses edited into each image. AGUIAR also notified CC-2 via WhatsApp that his friend had recommended a person to alter driver's licenses for $40.

100.   AGUIAR sent GUIMARAES NETO payments of $40 via Zelle corresponding to each license he asked him to edit. In total, between on or about October 16, 2019 and on or about November 8, 2019, AGUIAR sent GUIMARAES NETO $720 via Zelle, all in $40 or $80 increments. Between on or about May 20, 2019 through on or about February 12, 2021, GUIMARAES NETO received Zelle payments totaling approximately $963 from CC-5, including multiple payments in $40 increments in or about September and October 2019, which I believe, based on the foregoing, were payments to edit licenses for CC-5. During this same period, GUIMARAES NETO also received approximately $3,900 in Zelle payments from CABRAL and approximately $2,740 in Zelle payments from another individual, Co-Conspirator 11 ("CC-11").[12] Between on or about May 20, 2019 and on or about February 12, 2021, GUIMARAES NETO sent approximately $27,415 to DA SILVEIRA via Zelle.

101.   GUIMARAES NETO and AGUIAR also discussed in these chats whether the edited licenses would be caught by Rideshare Company A or Rideshare Company C's respective

---

[12] I am aware from my review of summary translations of WhatsApp chats that CC-2 shared with CC-11 that CC-2 purported to have someone who would edit licenses for $40. I believe, based on the foregoing, that CC-2 was referring to GUIMARAES NETO.

fraud detection systems.   For example, on or about November 1, 2019, AGUIAR sent GUIMARAES NETO a message from Rideshare Company C that an account had been suspended. AGUIAR also gave GUIMARAES NETO tips about how to manipulate the angles from which the photographs were taken in order for Rideshare Company A to accept them.

102.   On or about October 30, 2019, GUIMARAES NETO inquired of AGUIAR, in substance, whether they were using the same source for Social Security numbers and whether they were paying the same price.

103.   GUIMARAES NETO also occasionally asked AGUIAR to obtain driver's licenses for him. For example, on or about November 1, 2019, GUIMARES NETO asked AGUIAR to obtain four driver's licenses for him for $50 total.

104.   I have also reviewed records for a Bank of America account in GUIMARAES NETO's name.   Between in or about December 2018 and in or about February 2021, GUIMARAES NETO received nearly $155,000 from the Rideshare/Delivery Companies. Of that amount, more than $48,000 was received in the names of approximately 31 drivers. During that same period, GUIMARAES NETO received approximately $234,094 in Zelle inflows.

Defendant J

105.   The investigation has revealed that, as part of the scheme, Defendant J bought and sold driver's licenses and Social Security numbers; edited driver's licenses; prepared and submitted applications using fraudulent identifiers; rented and sold fraudulent driver accounts; referred prospective drivers to AGUIAR; and exchanged information with other conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection systems.

106.   Defendant J   communicated with AGUIAR via WhatsApp using the phone number ████████ (the "Defendant J   TELEPHONE"). This number is associated with

a Zelle account in Defendant J   's name, which is in turn linked to a Bank of America account

in Defendant J   's name, for which Defendant J   is also listed as having the ^{Defendant J}

phone. AGUIAR identified the ███████████ phone number as "^{Defendant J} Califa Zelle." I

believe "Califa" refers to "California," where Defendant J   resided.

107.   I have reviewed a draft summary translation of a chat between Defendant J

and AGUIAR, as well as computer-generated translations of chats between AGUIAR and

individuals Defendant J   referred to AGUIAR. For example, on or about November 13,

2019, AGUIAR asked Defendant J   , via WhatsApp, whether he knew anyone interested in

an account with Rideshare Company C.   Later that day, ^{Defendant K} contacted AGUIAR over

WhatsApp to rent the account. During the chat between AGUIAR and ^{Defendant K}, AGUIAR asked

^{Defendant K} if "^{Defendant J}" had discussed the rental cost with him, and informed ^{Defendant K} it was $300 per

week. In another instance, on or about April 25, 2020, a driver contacted AGUIAR for an account

with Delivery Company E, and AGUIAR confirmed that "^{Defendant J}" had told him the driver would be

contacting him.

108.   Defendant J   also managed his own fraudulent driver accounts. In or about

November 2019, Defendant J   and AGUIAR complained to one another, in substance, about

losses they incurred when the Rideshare/Delivery Companies suspended the fraudulent accounts
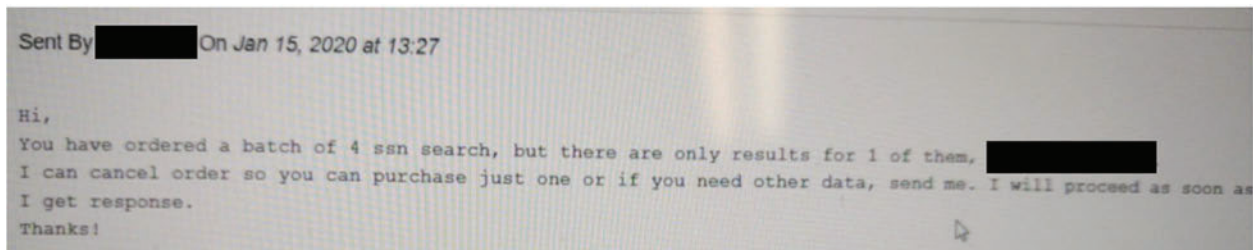
that they managed.

109.   Defendant J   and AGUIAR also exchanged driver's licenses and Social

Security numbers. For example, on or about November 24, 2019, Defendant J   sent

AGUIAR an image of a driver's license for which Defendant J   needed the corresponding

Social Security number. AGUIAR agreed, in substance, to ask his source for Social Security

numbers on the DarkNet. On or about the next day, Defendant J   asked AGUIAR if another

individual, Co-Conspirator 12 ("CC-12"), was his source for Social Security numbers. AGUIAR

replied, in substance, that he had dealt with CC-12 in the past, but no longer used him. ^{Defendant J}

and AGUIAR also discussed what happened when they applied for driver accounts

without a Social Security number.

110.   Defendant J   and AGUIAR also discussed the prices they paid for Social

Security numbers. Subsequently, on or about December 27, 2019, Defendant J   offered to

provide AGUIAR with Social Security numbers at a better price than what AGUIAR was getting

from his existing source. On or about January 13, 2020, Defendant J   told AGUIAR he

would charge him $60 per Social Security number. Thereafter, AGUIAR sent Defendant J

victims' driver's licenses and requested Social Security numbers. Two days later, ^{Defendant J}

sent AGUIAR a photo of the following message from his source, which was in English

and which I have redacted, notifying him that of the four Social Security numbers he had requested,

only one was available:


```
Sent By          On Jan 15, 2020 at 13:27

Hi,
You have ordered a batch of 4 ssn search, but there are only results for 1 of them,
I can cancel order so you can purchase just one or if you need other data, send me. I will proceed as soon as
I get response.
Thanks!
```

111.   I believe, based on my knowledge of the investigation, that Defendant J

edited driver's licenses. For example, on or about February 15, 2020, approximately one month

after Defendant J   expressed his interest in entering the Boston market, Defendant J

notified AGUIAR that he was having a template of a Massachusetts driver's license made.

Defendant J   asked AGUIAR to take a high-quality photo of a Massachusetts driver's license

for Defendant J   to use in the template.

112.   On or about February 20, 2020, Defendant J   sent AGUIAR photos of licenses he had edited, and AGUIAR provided feedback on the shading. During this exchange, AGUIAR sent Defendant J   a template for vehicle insurance.

113.   Throughout their chats, Defendant J   and AGUIAR exchanged tips about how to avoid the Rideshare/Delivery Companies' fraud detection systems. For example, on or about December 9, 2019, Defendant J   shared a tip about taking a picture of a picture to get past Rideshare Company C's fraud detection system. On or about January 19, 2020, Defendant J instructed AGUIAR to apply for accounts via Rideshare Company C's website, as opposed to its app, for better results.

114.   AGUIAR also told Defendant J   that he was working with others. For example, on or about December 4, 2019, AGUIAR told Defendant J   that he and his partner had applied for 25 accounts with Rideshare Company A that week.

115.   On or about December 6, 2019, Defendant J   shared with AGUIAR a photograph of a GPS "spoofing" application he had purchased. On or about December 16, 2019, Defendant J   instructed AGUIAR about how the application worked.

116.   I have also reviewed records for a Bank of America account in Defendant J   's name. Between in or about September 2019 and in or about February 2021, Defendant J received approximately $41,000 from the Rideshare/Delivery Companies in the names of approximately 47 drivers.

117.   Defendant J   is listed in corporation records filed with the State of California as the Chief Executive Officer, Secretary, Chief Financial Officer, and Director of ██████████, a company incorporated in California in or about October 2020. Defendant K is listed as the sole other Director. The type of business is "ecommerce."

118.   I have reviewed bank records for ▇▇▇▇. Based on my training and experience and my knowledge of the investigation, I believe ▇▇▇▇ was set up to launder money associated with the Rideshare/Delivery Company scheme. More than $75,000 has been passed through ▇▇▇▇ since it was incorporated in or about October 2020, more than $13,000 of which comprised Zelle transfers from Defendant J . Another approximately $21,000 was deposited into the account in seven cash transactions, all in amounts less than $10,000.

Defendant K

119.   The investigation has revealed that, as part of the scheme, $^{\text{Defendant K}}$ created or caused to be created multiple driver accounts with his image; referred a potential conspirator to AGUIAR; laundered money through ▇▇▇▇. with Defendant J ; and exchanged information with other conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection systems.

120. $^{\text{Defendant K}}$ communicated with AGUIAR via WhatsApp using the phone number ▇▇▇▇ (the "$^{\text{Defendant K}}$ TELEPHONE"). I have reviewed a computer-generated translation of this chat. During the chat, $^{\text{Defendant K}}$ sent AGUIAR his bank information, which matches a Wells Fargo account ending in ▇▇ in $^{\text{Defendant K}}$'s name. $^{\text{Defendant K}}$ also sent "selfie" photographs of himself. Additionally, $^{\text{Defendant K}}$sent AGUIAR screenshots showing Zelle payments he made to AGUIAR, which correspond to Zelle payments drawn on $^{\text{Defendant K}}$'s bank account. AGUIAR also saved the $^{\text{Defendant K}}$ TELEPHONE in his contacts under the name "$^{\text{Defendant K}}$ [Rideshare Company C] Califa." I believe "Califa" refers to "California," where $^{\text{Defendant K}}$ resided.

121.   As described above, $^{\text{Defendant K}}$ contacted AGUIAR at the recommendation of his friend "$^{\text{Defendant J}}$" for an account with Rideshare Company C. Additionally, Rideshare Company A's

records reflect four accounts created in the names of other individuals but bearing ^{Defendant K}'s

image.

122.   I have reviewed bank and Zelle records for ^{Defendant K}. Between on or about June

28, 2019 and on or about December 28, 2020, ^{Defendant K} received approximately $70,515 in

payments from various Rideshare/Delivery Companies in the names of at least 32 different

individuals. He also received Zelle transfers of approximately $135,483 during that period,

including approximately $23,224 from Defendant J   .[13]

123.   Additionally, on or about November 21, 2019, ^{Defendant K} told AGUIAR in a chat

that he had a contact who would edit driver's licenses for AGUIAR for $30 each.

Defendant L

124.   The investigation has revealed that, as part of the scheme, ^{Defendant L} acted as a

middleman between AGUIAR and individuals who rented fraudulent driver accounts. ^{Defendant L}

also managed accounts and collect payments from drivers; and exchanged information with other

conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection

systems. ^{Defendant L} also obtained at least one license for use in creating a fraudulent driver

account.

125.   ^{Defendant L} communicated with AGUIAR via WhatsApp using the phone number

████████████ (the "^{Defendant L} TELEPHONE"). The ^{Defendant L} TELEPHONE is associated with

---

[13] ^{Defendant K} also transferred approximately $17,132 to Defendant J   during this
period. I am aware that public records available to law enforcement list the same address for both
Defendant J   and ^{Defendant K} in Daly City, California. Based on my knowledge of the
investigation, I believe ^{Defendant K} and Defendant J   were roommates, and some of these Zelle
payments may have been associated with household expenses.

an insurance claim made by ^{Defendant L}.

126.   I have reviewed a draft summary translation of the chat between ^{Defendant L} and AGUIAR. In the chat, ^{Defendant L} shared a photograph of his own driver's license and vehicle registration with AGUIAR. Additionally, AGUIAR identified the contact using the ^{Defendant L} TELEPHONE as "^{Defendant L} Drive Califa." I believe "Califa" is a reference to "California," where ^{Defendant L} resided.

127.   On or about November 7, 2019, AGUIAR offered to work with ^{Defendant L} in connection with creating fraudulent driver accounts with Rideshare Company A and Rideshare Company C. AGUIAR proposed, in substance, to send photos of victims' driver's licenses to ^{Defendant L} so that ^{Defendant L} could find drivers with a similar appearance to use fraudulent accounts created in the victims' names. ^{Defendant L} confirmed that he knew people interested in renting accounts, but wanted to be paid more than he was receiving under a similar agreement with a conspirator. ^{Defendant L} and AGUIAR negotiated the price, and ^{Defendant L} agreed that he would be responsible for solving account problems, collecting payments from drivers, and managing the accounts in exchange for his commission.

128.   During this communication, ^{Defendant L} asked AGUIAR if he worked with CC-12. AGUIAR denied that he worked with CC-12, and confirmed that he his partner were willing to work with ^{Defendant L}. Based on my knowledge of the investigation, I believe the "partner" to which AGUIAR referred was CC-2.

129.   Thereafter, at AGUIAR's direction, ^{Defendant L} sent AGUIAR passport-style photos and "selfie" photos of drivers, along with vehicle registrations and proof of automobile insurance. In exchange, AGUIAR created fraudulent accounts for the drivers in the names of victims. Once

the accounts were set up, ^{Defendant L} sent AGUIAR the drivers' banking information so they could receive payments directly from Rideshare Company A and Rideshare Company C.

130.   In or about December 2019, ^{Defendant L} and AGUIAR discussed a driver who was late in paying his weekly rental fee. AGUIAR changed the password on the driver's account to prevent the driver from accessing it. AGUIAR told ^{Defendant L} that the individual to whom he reported controlled all account activities and pressured him to collect weekly payments from drivers.

131.   ^{Defendant L} and AGUIAR also discussed the cost to purchase (as opposed to rent) accounts. AGUIAR told ^{Defendant L}, in substance, that the $2,000 he charged for accounts was justified because he relied on a team to complete the work and outsourced various jobs, including the procurement of driver's licenses and Social Security numbers and editing licenses.

132.   In the course of their chats, ^{Defendant L} and AGUIAR exchanged tips about how to avoid the Rideshare/Delivery Companies' fraud detection systems. For example, on or about November 8, 2019, ^{Defendant L} told AGUIAR to apply for driver accounts in San Francisco, because they were going through more easily. ^{Defendant L} and AGUIAR also exchanged messages about how to resolve issues with account shutdowns, how to change banking information on a driver's account, and whether to use female names for male drivers because of a shortage of male accounts.

133.   On or about November 22, 2019, ^{Defendant L} told AGUIAR that his own driver account with Rideshare Company A had been shut down, and asked AGUIAR to create an account with Delivery Company B for him using a female victim's driver's license that ^{Defendant L} had obtained after a traffic accident in which he took a photo of the driver's license of the woman who hit him. AGUIAR suggested that he and ^{Defendant L} save this driver's license to use for an account

with Rideshare Company A instead. AGUIAR then suggested, in substance, that Defendant L

intentionally hit a car, preferably driven by an American male, in order to obtain a photograph of

his driver's license and use it for Defendant L's account. On or about November 27, 2019, Defendant L

shared with AGUIAR another fraudulent scheme to obtain driver's licenses involving liquor

deliveries.

134.   Thereafter, in or about December 2019, Defendant L sent AGUIAR an image of

Victim 17's driver's license, and on or about December 22, 2019, AGUIAR sent back a stock

photo of the same license resting on a wallet with Defendant L's photo edited onto the license.

AGUIAR and Defendant L thereafter exchanged screenshots concerning a Rideshare Company A

account in Victim 17's name featuring Defendant L's photo.

135.   I have reviewed bank records for Defendant L's account at Wells Fargo. Between on

or about November 3, 2019 and on or about June 9, 2020, Defendant L received approximately

$43,167 in deposits into his Wells Fargo account ending in ▆▆▆. Zelle transfers comprised

approximately $33,515 of that amount. Many of those deposits were in amounts of $200 or $250,

paid weekly from various individuals. These transfers often referenced "[Rideshare Company A]"

or "Conta," which is the Portuguese word for "account."   Based on my knowledge of this

investigation, I believe that many of these transfers were from individuals renting or buying

fraudulent driver accounts.

BRUNO PROENCIO ABREU

136.   The investigation has revealed that, as part of the scheme, ABREU supplied

BARBOSA with driver's license images and assisted BARBOSA with obtaining Social Security

numbers from the DarkNet.

137.   ABREU communicated with BARBOSA via text message and WhatsApp using the phone number 774-204-2552 (the "ABREU TELEPHONE"). I have reviewed a draft summary translation of these messages and chat. In the chat, ABREU sent pictures of himself to BARBOSA. Additionally, payments they discussed correspond to payments reflected in bank statements for an account in ABREU's name. BARBOSA saved the ABREU TELEPHONE in her contacts under the name "Bruno," which is ABREU's first name.

138.   ABREU supplied BARBOSA with driver's license images that BARBOSA used to open fraudulent driver accounts. Between in or about October 2020 and in or about January 2021, ABREU sent BARBOSA more than 90 driver's license images. For example, on or about October 21, 2020, ABREU sent BARBOSA an image of the driver's license of Victim 18. BARBOSA'S bank statements indicate that BARBOSA received a deposit of $1,000 from Delivery Company D, referencing Victim 18, on or about November 10, 2020. I believe this payment may have been a referral bonus based on the creation of a driver account in Victim 18's name.

139.   Similarly, on or about October 21, 2020, ABREU sent BARBOSA an image of Victim 19's driver's license. BARBOSA'S bank statements indicate that BARBOSA received a deposit of $500 from Delivery Company D, referencing Victim 19, on or about November 10, 2020. I believe this payment was also a referral bonus based on the creation of a driver account in Victim 19's name.

140.   Based on my knowledge of the investigation and review of the license images ABREU sent BARBOSA, I believe that ABREU obtained the images of the driver's licenses of Victim 18 and Victim 19, and of other victims, while delivering alcohol orders for one or more of the Delivery Companies, by falsely telling the delivery recipients that the Delivery Company required him to take a photograph of their licenses in order to verify the recipient's date of birth.

45

Specifically, many of the photos show victims holding up their licenses to the camera, often through a doorway or on a porch. I have also reviewed a WhatsApp chat between BARBOSA and LIMA GUIMARAES, in which BARBOSA indicated, in substance, that she sent ABREU to make deliveries from a liquor store in Connecticut in order to procure images of Connecticut licenses.

141.   ABREU, who lives with BARBOSA at 1205 Rock Wood Drive, Saugus, Massachusetts, also helped BARBOSA find Social Security numbers. For example, on or about November 18, 2019, ABREU agreed to help BARBOSA use Bitcoin to purchase Social Security numbers on a DarkNet site she had located. In other WhatsApp messages from in or around November 2019, ABREU and BARBOSA discussed alternative sources for Social Security numbers. In one message, ABREU suggested to BARBOSA that they partner with an accountant who might have direct access to Social Security numbers through a government database.

142.   I have reviewed records for a Bank of America account in ABREU'S name. Between in or about December 2018 and in or about December 2020, ABREU received approximately $51,484 from the Rideshare/Delivery Companies, including payments of approximately $10,641 referencing the names of at least 18 other individuals. BARBOSA's Venmo records reflect that she paid ABREU approximately $5,276 in 2020.

JORDANO AUGUSTO LIMA GUIMARAES

143.   The investigation has revealed that, as part of the scheme, LIMA GUIMARAES supplied BARBOSA with driver's license images; referred other drivers to her; and exchanged information with BARBOSA about sources for driver's licenses.

144.   LIMA GUIMARAES communicated with BARBOSA via WhatsApp using the phone number 857-888-2714 (the "LIMA GUIMARAES TELEPHONE"). I have reviewed a draft summary translation of this chat. During the chat, LIMA GUIMARAES sent a photograph of

himself. Additionally, BARBOSA saved the LIMA GUIMARAES TELEPHONE in her contacts

under the name "Jordano," which is LIMA GUIMARAES's first name.

145.   In or around August 2020, LIMA GUIMARAES asked BARBOSA to create a

driver account for him and sent BARBOSA a "selfie." BARBOSA created an account for LIMA

GUIMARAES in Victim 20's name and sent LIMA GUIMARAES a photograph of Victim 20's

license edited to show LIMA GUIMARAES's photo. According to their messages, LIMA

GUIMARAES began using the fraudulent account later the same day.

146.   In or about September 2020, LIMA GUIAMARAES contacted BARBOSA again

to request an additional driver account. LIMA GUIMARAES told BARBOSA, in substance, that

he had a victim's driver's license already and sent it to BARBOSA. BARBOSA opened a

fraudulent driver account for LIMA GUIMARAES that same day, and LIMA GUIMARAES

offered to send BARBOSA additional driver's license images that he and his spouse collected in

the future.

147.   Days later, LIMA GUIMARAES contacted BARBOSA and, in substance, agreed

to send her additional driver's licenses in exchange for payment. LIMA GUIMARAES then sent

BARBOSA photographs of three driver's licenses. For the reasons set forth above, I understand

these photographs to have been taken in connection with alcohol deliveries for one of the Delivery

Companies. BARBOSA replied that she already had an image of one of the driver's licenses.

148.   On or about October 3, 2020, BARBOSA contacted LIMA GUIMARAES for

additional driver's licenses.   The following day, LIMA GUIMARAES sent BARBOSA

photographs of three additional driver's licenses that appear to have been taken during deliveries.

Over the following month, LIMA GUIMARAES sent BARBOSA photographs of at least 30

additional Massachusetts driver's licenses. BARBOSA paid LIMA GUIMARAES following each

transmission of photographs of licenses. LIMA GUIMARAES subsequently began sending BARBOSA photographs of driver's licenses by text message instead of WhatsApp. Between in or about October 2020 and in or about January 2021, LIMA GUIMARAES texted BARBOSA over 150 images of driver's licenses.

149.   LIMA GUIMARAES's driver accounts were deactivated in or about December 2020, but BARBOSA created two additional accounts using his image on victims' driver's licenses.

150.   LIMA GUIMARAES also referred other drivers to BARBOSA for obtaining fraudulent accounts with the Rideshare/Delivery Companies. In substance, LIMA GUIMARAES and BARBOSA discussed how much she would charge to create an account for a friend of LIMA GUIMARAES who could supply an image of a victim's driver's license to BARBOSA.

151.   LIMA GUIMARAES and BARBOSA also discussed ways to obtain additional driver's licenses. For example, BARBOSA told LIMA GUIMARAES that she sent her roommate to Connecticut to procure driver's licenses and that he delivered for a wine shop there. LIMA GUIMARAES expressed interest in doing the same, and later told BARBOSA that he had asked some of his friends from Connecticut to get driver's licenses for him.

152.   I reviewed records of a Bank of America account for LIMA GUIMARAES indicating that, between September 2020 and January 2021, BARBOSA sent GUIMARAES approximately $5,100 via Zelle.

Defendant O

153.   The investigation has revealed that, as part of the scheme, Defendant O supplied BARBOSA with driver's license images and exchanged information with her regarding account deactivations.

154.   Defendant O communicated with BARBOSA via text message and WhatsApp using the phone number ███████ (the "Defendant O TELEPHONE"). I have reviewed a draft summary translation of this chat. The profile photo associated with the Defendant O TELEPHONE on WhatsApp appears to be a photo of Defendant O based on my review of known photographs of Defendant O. In the chat, the person using the Defendant O TELEPHONE sent a screenshot of a bank account and routing number that matches Defendant O's bank account. Additionally, BARBOSA saved the Defendant O TELEPHONE in her contacts under the name "Defendant O," which is Defendant O'S first name.

155.   Between in or about November 2020 and in or about January 2021, Defendant O sent BARBOSA more than 75 driver's license images. In numerous WhatsApp exchanges, Defendant O and BARBOSA discussed the quality of the images and whether any of the images were duplicates of images BARBOSA already had. In one exchange, BARBOSA indicated to Defendant O that Defendant O was one of two suppliers of driver's licenses that BARBOSA used at the time. It is apparent from the chat that Defendant O obtained driver's license images from victims to whom he delivered alcohol. For example, BARBOSA and Defendant O discussed, in substance, that BARBOSA needed driver's licenses to fulfill 20 requests for new accounts, but Defendant O had none because he had not delivered a single order for alcohol that day.

156.   Defendant O and BARBOSA also exchanged numerous messages about Delivery Company E's deactivation of accounts that BARBOSA rented to drivers. For example, Defendant O explained to BARBOSA that Delivery Company E likely deactivated certain accounts BARBOSA had rented as part of an annual, year-end clean-up. In another exchange, BARBOSA and Defendant O speculated that certain driver's licenses obtained by Defendant O might have already been used in the creation of other fraudulent accounts.

157.   I have reviewed records for a Bank of America account in Defendant O's name. Between in or about December 2018 and in or about December 2020, Defendant O received approximately $34,271 from the Rideshare/Delivery Companies. Of that amount, approximately $34,019 was in the names of approximately 20 drivers.

158.   Additionally, Zelle account statements reflect payments of approximately $1,355 from BARBOSA to Defendant O between November and December 2020, which I believe, based on my knowledge of the investigation, comprised payments for the driver's license images that Defendant O provided.

ALESSANDRO FELIX DA FONSECA

159.   The investigation has revealed that, as part of the scheme, DA FONSECA referred drivers to BARBOSA; managed accounts for BARBOSA; collected referral bonuses; and exchanged information with other conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection systems.

160.   DA FONSECA communicated with BARBOSA via WhatsApp using the phone number 857-346-8771 (the "DA FONSECA TELEPHONE"). I have reviewed a computer-generated translation of this chat. In the chat, DA FONSECA and BARBOSA share screenshots of payments confirming that they sent funds to each other. I have reviewed bank records in their names that reflect corresponding transfers into their accounts. Additionally, BARBOSA saved the DA FONSECA TELEPHONE in her contacts under the name "Ale Carro." I believe "Ale" is short for "ALESSANDRO," which is DA FONSECA's first name, and "Carro" is the Portuguese word for "car."

161.   DA FONSECA provided support for BARBOSA's account creation services. For example, in or about November 2019, DA FONSECA sent BARBOSA several drafts of an

advertisement to attract drivers to the scheme, and BARBOSA edited the drafts. After BARBOSA

approved the advertisement, DA FONSECA indicated that he had posted it and that several

individuals had contacted him. DA FONSECA asked for BARBOSA's price list, and BARBOSA

responded with weekly rental rates for each Rideshare/Delivery Company for accounts using an

unedited image of a victim's driver's license and accounts using an image of a driver's license

edited to depict the driver's photo. DA FONSECA subsequently directed individuals to

BARBOSA for account rentals and forwarded their names and bank account information to

BARBOSA to use in creating accounts. In return, BARBOSA sent DA FONSECA the login

information for the drivers to use.

162.   DA FONSECA and BARBOSA also coordinated to link debit cards associated with

the Delivery Company D accounts they created to bank accounts. Based on my knowledge of the

investigation, I know that Delivery Company D provides drivers with a debit card to use to

purchase the items that drivers pick up and deliver for Delivery Company D's customers. DA

FONSECA instructed BARBOSA to have activation kits containing these debit cards sent to

specified addresses, and he sent BARBOSA photographs of the debit cards and screenshots of the

bank account information to be linked to the cards.

163.   DA FONSECA and BARBOSA also coordinated to receive referral bonuses from

the Rideshare/Delivery Companies in connection with the creation of fraudulent driver accounts

and communicated with each other about account deactivations and other issues. For instance, on

or around December 23, 2019, BARBOSA told DA FONSECA, in substance, that Rideshare

Company A had deactivated 75% of her accounts, which she suspected were accounts where the

Social Security number she had purchased did not actually correspond to the victims' identities.

The same day, DA FONSECA told BARBOSA he was looking at the "bills," and BARBOSA sent

him images of Delivery Company D's app opened to the referral page, showing delivery progress and referral bonus amounts for various names under which they had opened accounts.

164. In or about July 2020, DA FONSECA sent BARBOSA a link to a news article about a Rideshare/Delivery Company and the availability of its customers' personal data online. DA FONSECA explained to BARBOSA that the news article referenced a DarkNet that sold information about Delivery Company E's customers. BARBOSA asked DA FONSECA if she should be concerned, and DA FONSECA told her, in substance, "No more than you already are."

165. I have reviewed statements from a Bank of America account for DA FONSECA which reflect payments from Rideshare/Delivery companies totaling approximately $77,011 between March 2019 and December 2020, including payments of approximately $45,761 referencing the names of at least 25 other individuals. The bank statements also reflect Zelle transfers from BARBOSA to DA FOSNECA during this period totaling approximately $12,000.

Defendant Q

166. The investigation has revealed that, as part of the scheme, Defendant Q prepared and submitted applications using fraudulent identifiers; rented and sold fraudulent driver accounts; managed accounts; referred potential drivers to BARBOSA; and exchanged information with other conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection systems.

167. Defendant Q communicated with BARBOSA and AGUIAR via WhatsApp at the telephone number ██████████ (the "Defendant Q TELEPHONE"). I have reviewed computer-generated translations of these chats. In the chat with BARBOSA, Defendant Q and BARBOSA shared screenshots confirming that they sent funds to each other. I have reviewed Bank of America records for BARBOSA that reflect

corresponding transfers to an account in Defendant Q   's name. Additionally,

BARBOSA listed the Defendant Q   phone as "^{Defendant Q}" in her contacts. AGUIAR listed

Defendant Q   as "^{Defendant Q} [Delivery Company B]" in his contacts.

168.   In or about December 2019, AGUIAR contacted Defendant Q   via

WhatsApp to see if he knew anyone interested in renting Delivery Company B accounts. There

was no indication of a response in AGUIAR's iCloud Account.

169.   In their WhatsApp chat, Defendant Q   and BARBOSA discussed, in

substance, that Defendant Q   was creating accounts for BARBOSA. For example, on

or about June 10, 2020, BARBOSA sent Defendant Q   an image of Victim 21's

driver's license and Social Security number, and a passport-style photo and a "selfie" photo of

another individual, Co-Conspirator 13 ("CC-13"), as well as a vehicle registration and inspection

report for a Toyota Prius registered to CC-13. Delivery Company B records confirm that an

account ("Account 21") in Victim 21's name was created on or about October 7, 2020 in the area

of Hartford, Connecticut. The vehicle associated with Account 21 was associated with six other

accounts, all created in or around Chelsea, Massachusetts or Boston, Massachusetts. One of the

accounts, in the name of Victim 22, used an insurance card with an address of 2 Fairmont Street,

Woburn, Massachusetts.   This address was also used in insurance documents on accounts

associated with AGUIAR. While the driver's license information is different on each of these

accounts, the photo on the license and the associated "selfie" of the driver are the same. These

same photos were used on three other Delivery Company B accounts created in the same locations

in Boston and Chelsea. One of these accounts, in the name of Victim 23, was referred by an

account in the name of Victim 24 ("Account 24"). The photo on the image of Victim 24's license

submitted to Delivery Company B and the accompanying "selfie" depict Defendant Q   .
Account 24 is linked to 129 other Delivery Company B accounts.

170.   On or about October 7, 2020, BARBOSA sent Defendant Q   images of
three victims' Massachusetts driver's licenses and their Social Security numbers to create
fraudulent accounts for her, and told Defendant Q   she had paid him for all three.
Venmo records reflect that, on or about October 6, 2020, BARBOSA paid Defendant Q
$750 from in or around Saugus, Massachusetts. On or about October 9, 2020,
Defendant Q   asked BARBOSA if she wanted to receive the rents for the accounts
directly, from which she could send him his share.

171.   On or about October 29, 2020, Defendant Q   sent BARBOSA a
screenshot of photos saved on his phone that appear to be victims' Social Security cards and
driver's license images.

172.   Defendant Q   also managed accounts for BARBOSA. For example, on
or about October 9, 2020, Defendant Q   sent BARBOSA an excerpt of a spreadsheet
reflecting victims' names, phone numbers, email addresses used to open accounts, Social Security
numbers, dates of birth, the first names of the drivers using the accounts, whether the accounts
were being rented or sold, the price, and whether the accounts were with Rideshare Company A
or Delivery Company B. Victim 21's name appears in the spreadsheet, as well as one of the victims
whose information BARBOSA sent Defendant Q   on or about October 7, 2020.
Defendant Q   gave BARBOSA regular updates on the status of the accounts.
Defendant Q   also sent BARBOSA screenshots of his conversations with drivers
renting the accounts to keep her updated on their status.

173.   Defendant Q   also referred prospective drivers to BARBOSA. For example, on or about October 9, 2020, Defendant Q   asked BARBOSA, in substance, if she had any Rideshare Company C accounts available for a friend in Florida.

174.   Defendant Q   also worked with another individual, CC-5, to obtain Social Security numbers for BARBOSA. For example, on or about October 16, 2020, Defendant Q   notified BARBOSA, in substance, that CC-5 was unable to locate the Social Security number corresponding to a victim whose a driver's license BARBOSA had sent Defendant Q   , but was able to locate the Social Security number for a different victim. Defendant Q   also referenced CC-5 on or about October 24, 2020, when he sent BARBOSA an updated spreadsheet tracking the accounts he managed for her, and added that he had not talked to CC-5 about the rental amounts listed in the spreadsheet.

175.   Defendant Q   also relayed information to BARBOSA about the Rideshare/Delivery Companies' fraud detection systems. For example, on or about October 21, 2020, Defendant Q   notified BARBOSA, in substance, that an account he had applied for the previous day had been terminated before the background check was completed and indicated that he was going to analyze what happened to figure out how to prevent accounts from being closed before they were opened. On or about October 31, 2020, Defendant Q   told BARBOSA that, prior to the COVID-19 pandemic, he would accompany a friend who had an account with Rideshare Company A to Rideshare Company A's local office to learn about how the company reviewed accounts.

176.   In a chat on or about October 26, 2020, Defendant Q   and BARBOSA discussed, in substance, who edited driver's licenses for them.

177.   Zelle and Venmo records confirm that, between in or about October 2020 and in or about November 2021, Defendant Q received approximately $2,800 from BARBOSA. Between in or about April 2020 and in or about December 2020, Defendant Q received approximately $9500 from CC-5. Between in or about November 2019 and in or about July 2020, Defendant Q received approximately $4,170 from Defendant R.

Defendant R

178.   The investigation has revealed that, as part of the scheme, Defendant R exchanged driver's licenses and Social Security numbers with BARBOSA and exchanged information with other conspirators about how to circumvent the Rideshare/Delivery Companies' fraud detection systems.

179.   Defendant R communicated with BARBOSA via WhatsApp using the phone number ███████ (the "Defendant R TELEPHONE"). The Defendant R TELEPHONE is associated with a Zelle account in Defendant R's name.

180.   I have reviewed a computer-generated translation of the chat between Defendant R and BARBOSA. In or about April 2020, Defendant R sought BARBOSA's help with a Delivery Company E account. Defendant R assured BARBOSA, in substance, that he would not "get in the way" of her work. Defendant R also asked BARBOSA about issues related to using a "bot" with one or more apps.

181.   Defendant R and BARBOSA also exchanged victims' driver's licenses and Social Security numbers. For example, in or about June 2020, Defendant R sent BARBOSA nine Illinois driver's license images, and BARBOSA replied with corresponding Social Security numbers. In connection with this exchange, Defendant R sent BARBOSA a Zelle transfer of $900.

182.   I reviewed bank statements for a Bank of America account for Defendant R.

Between in or about December 2018 and in or about December 2020, Defendant R received

deposits totaling more than $102,000 from Rideshare/Delivery Companies, including payments of

more than $51,000 in the name of at least 33 other individuals. Defendant R also received over

$258,000 in Zelle transfers, including recurring payments from several individuals, such as

Defendant Q   , in amounts consistent with the rental of accounts.

THE PREMISES CONTAIN EVIDENCE, FRUITS, AND INSTRUMENTALITIES

183.   I also have probable cause to believe that the premises contain fruits, evidence, and

instrumentalities of violations of the TARGET OFFENSES, as described in Attachment B.

184.   On or about April 5, 2021, the Honorable Judith G. Dein issued a warrant for precise

location information (GPS E-911 data) with respect to the mobile phone assigned number 207-

300-3003, used by BARBOSA, for which T-Mobile is the service provider. Information from that

warrant has regularly placed BARBOSA in the vicinity of the BARBOSA/ABREU RESIDENCE

for the past month, including during overnight hours. Investigators have conducted surveillance

over the past month and observed BARBOSA and ABREU outside the BARBOSA/ABREU

RESIDENCE and vehicles registered to them in the driveway.   Additionally, the

BARBOSA/ABREU RESIDENCE is listed as the mailing address on BARBOSA's bank

statements. In WhatsApp chats with other conspirators, BARBOSA has stated, in substance, that

her roommate obtains driver's licenses for her, which corresponds to ABREU's activity in the

scheme.

185.   In a directory dated as of April 23, 2021, the management company for the DA

SILVA RESIDENCE listed DA SILVA and an individual believed to be DA SILVA's spouse as

the current residents of the DA SILVA RESIDENCE. The DA SILVA RESIDENCE is listed on

an identification for DA SILVA issued by the Massachusetts Registry of Motor Vehicles. DA SILVA has a Toyota Prius registered in his name at the DA SILVA RESIDENCE. Investigators have conducted physical surveillance over the past month and observed that vehicle parked in different spots outside of the DA SILVA RESIDENCE on at least three separate occasions, including during overnight hours. Based on my training and experience, I am aware that individuals often spend overnight hours in their own residence, and will leave their vehicle parked outside their residence overnight. While investigators have not yet observed DA SILVA at the residence, I am aware from my involvement in this investigation that DA SILVA does not hold a regular, "9-5" job, and keeps irregular hours. Public records available to law enforcement also list the DA SILVA RESIDENCE as the likely residence for DA SILVA. Specifically, these records reflect that Experian identified the DA SILVA RESIDENCE as the most reliable of the possible addresses for DA SILVA.

186. From my training and experience, I know that locations occupied by a target will contain evidence that will aid in establishing the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. I believe it is likely that the BARBOSA/ABREU RESIDENCE and DA SILVA RESIDENCE will contain evidence of the TARGET OFFENSES, including, without limitation, computers and cell phones used in the offense, including those used to create accounts, send or receive payments, track accounts, and communicate with conspirators; debit cards and welcome kits mailed by the Rideshare/Delivery Companies; records of driver accounts created, victim personal identifying information, drivers renting accounts, payments made or received in connection with the scheme, or concerning Bitcoin purchases or the transfer of funds to bank accounts in Brazil; and cash.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

187.   From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through email, instant messages, and updates to online social networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

188.   Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence that reveals or suggests who possessed or used the device.

189.   Here, the defendants communicated with each other and other conspirators via WhatsApp and text message. They used their phones and computers to obtain driver's licenses and Social Security numbers, edit driver's licenses, create driver accounts with the Rideshare/Delivery Companies, rent or sell accounts, advertise their scheme, coordinate on pricing, purchase "bots" and GPS "spoofing" technology, share tips about how to circumvent the Rideshare/Delivery Companies' fraud detection systems, refer other drivers to the scheme, and transfer money.

190.   Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a.   Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b.   Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c.   Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d.   Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often

maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

191.   As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is

analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crimes under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

192.   A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

193.   The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

194.   Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

195.   Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a.   The volume of evidence that storage media such as hard disks, flash drives, CDs, and DVDs can store is the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis onsite.

b.   Technical requirements analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

196.   The Premises may contain computer equipment whose use in the crimes or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In

addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

197.   The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B because they are associated with (that is used by or belong to) BARBOSA, ABREU, or DA SILVA. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

198.   This warrant authorizes a review of electronically stored information, communications, other records, and information seized, copied or disclosed pursuant to this warrant to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNLOCKING A DEVICE USING BIOMETRIC FEATURES

199.   I know from my training and experience, as well as from information found in publicly available materials, that some models of cellphones made by Apple and other manufacturers offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

200.   On the Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to five fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used instead, such as: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

201.   The passcode that would unlock device(s) found during the search of the Subject Premises is not currently known to law enforcement. Thus, it may be useful to press the finger(s) of the user(s) of the device(s) to the device's fingerprint sensor or to hold the device up to the face of the owner in an attempt to unlock the device for the purpose of executing the search authorized by this warrant. The government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

202.   In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it may be necessary for law enforcement to have the ability to require any occupant of the Subject Premises to press their finger(s) against the sensor of the locked device(s) or place the devices in front of their faces in order to attempt to identify the device's user(s) and unlock the device(s).

203.   For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the Premises to the sensor of the devices or place the devices in front of their faces for the purpose of attempting to unlock the device to search the contents as authorized by this warrant.

CONCLUSION

204.   Based on my knowledge, training, and experience, and the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that defendants conspired to commit wire fraud, in violation of Title 18, United States Code, Section 1349.

205.   Based on my training and experience and the facts set forth above, I believe there is also probable cause to believe that evidence, fruits, and instrumentalities of these crimes, as described in Attachment B, are contained within the premises described in Attachments A-1 and A-2.

Sworn to under the pains and penalties of perjury,

Terrence Dupont
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on May 6, 2021 by telephone

_____
Hon. Judith G. Dein
United States Magistrate Judge